

## **REMARKS**

This Amendment is being filed in response to the outstanding Office Action, dated July 10, 2002 in which the Examiner rejected claims 1-21, all of the claims currently pending in the subject application. Applicants notes that the amendments to the claims have been made to clarify the invention and, other than removing the typographical error in claim 20, were not made to address the rejections made by the Examiner.

Attached hereto is a mark-up version of the changes made to the claims by the current amendment. The attached page is entitled “**VERSION WITH MARKINGS TO SHOW CHANGES**”.

### **Examiner’s Objections to the Claims**

Prior to turning to the substantive rejections, Applicant addresses the Examiner’s objection to claim 20. The Examiner objected to claim 20 in that claim 20 appears to have contained a typographical error. Specifically, the phrase “a+ merchant” was presumed by the Examiner to be a typographical error.

Applicant has amended claim 20 to remove the “a+” from claim 20. Applicant submits that the amendment addresses the Examiner’s objections and respectfully requests that the Examiner withdraw the objection to claim 20.

### **Rejections Under 35 U.S.C. § 103(a)**

The Examiner rejected claims 1-6, 8-17, and 20-21 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,670,717 (“Wiecha”) in view of U.S. Patent No. 5,982,891 (“Ginter”). Applicant respectfully traverses the rejection in light of the amendments and arguments made herein.

With reference to independent claims 1, 11, 14, 17, and 20, the Examiner contends that the Wiecha patent discloses a service and system containing a purchase to database with identifier and address for a purchase order and processor for receiving purchase order from network 34 using the identifier. The Examiner, however, concedes that the Wiecha patent fails to disclose a “disabler”. Nevertheless, the Examiner contends that the Ginter patent discloses a disabler to disable the account when tampering occurs and that it would be obvious to one skilled in the art at the time of the invention to modify the system of the Wiecha patent to have the

disabler of the Ginter patent to secure the personal information of the participants in systems transactions. Applicant respectfully traverses this rejection on the ground that neither Wiecha nor Ginter disclose the features of independent claims 1, 11, 14, 17, and 20.

Wiecha describes a corporate purchasing system where a vendor catalog is stored locally on a corporate network in which an employee selects items from the local catalog and submits the selected items to a manager for approval. See Wiecha col. 3, lines 10-37. Orders are fulfilled in a normal manner. Id. at col. 3, lines 42-43. In other words, a corporate entity either pays for the selected items using a pre-established corporate account with a particular vendor or some other form of payment such as electronic wire transfer or credit card payment. In either payment scenario, the vendor has access to the corporate entity's payment information, such as a credit card number.

In contrast, the subject application is directed to a separate purchasing processing system that securely stores a user's payment information, such as credit or debit card number, and can in response to receipt of a purchase order (or request for payment) from a merchant fulfill the order by effectuating payment to the merchant without exposing the consumer's payment information to the merchant, as set forth in claims 1, 11, 14, 17, and 20. See Specification at pg. 5, lines 7-15. Because Wiecha fails to teach or suggest such a system and method, Wiecha cannot properly serve as a base reference for an obviousness rejection.

Moreover, the purchasing processing system of the present application provides an additional layer of security not found in the cited references in that purchased goods can only be delivered to a delivery address stored in the purchaser account on the purchasing processing system. The purchasing processing system comprises a disabler for monitoring the status of the stored purchaser account information. If the disabler detects either unauthorized access (e.g., a hacker breaks into the purchaser account) or, even if an authorized user makes a change to the stored delivery address, then the associated purchaser identifier is disabled. As set forth in the specification of the present application, as originally filed:

A unique purchaser identifier is assigned to each purchaser and linked to that purchaser's purchasing information which is stored in a purchaser account. The identifier – or personal identification number (PIN)—bears no relation to the purchaser's financial

information. Only the identifier and the corresponding delivery information is communicated when purchases are made.

See Specification at pg. 5, lines 16-19. Further, it is explained that:

Furthermore, the purchaser identifier and the corresponding purchaser account cannot be changed at any time or by any party, including the purchaser, without that particular purchaser identifier and account being disabled. Once disabled the purchaser identified is void and a new identifier must be issued. The present invention, therefore, prevents unauthorized use of a purchaser's purchasing information by ensuring that any purchases are delivered only to the purchaser's physical or electronic address. Any fraudulent use of the purchaser identifier will be instantly revealed because the goods or electronic information must be delivered directly to the purchaser's delivery address. Because the purchaser will know whether a valid purchase has been made, the purchaser can suspend or disable the account without canceling credit or debit cards.

See Specification at page 6, lines 4-13.

Thus, even if the purchaser identifier is stolen and used to attempt a fraudulent purchase, the products will be delivered only to the pre-defined delivery address associated with that identifier. In this way, fraudulent purchases will be recognized immediately by the user who can notify his/her credit card company, for example, to stop payment. If any attempt to change the delivery address is made, the account will be disabled. Wiecha thus fails to teach or suggest the features of the claimed invention.

Similarly, Ginter fails to teach or suggest the disabler of the present invention. In contrast to the present invention, the "disabler" described in the Ginter reference is merely a general software process for a system operation. As such, Ginter does not teach or suggest a disabler to disable the purchaser account in response to any attempted change to the stored delivery data. See Specification at pg. 7, lines 9-12. In this way, unlike the references cited by the Examiner, the purchaser has complete control over where purchases are delivered and someone stealing the purchaser's account identifier (e.g., a user ID, password, or PIN number) would be unable to change the delivery address. Consequently, even if the purchaser identifier is stolen, the purchased article or piece of data or information, such as by way of example, an online software purchase or so called e-book, the purchaser will receive that purchase at his or

her specified delivery address and will thereby have notification of fraudulent use of his or her account. These features are neither taught or suggest by either the Wiecha or Ginter patents. As such, applicant submits that claims 1, 6, and 14 and those claims depending therefrom adequately distinguish from the cited references and are therefore in condition for allowance.

With reference to claims 8 and 11, which the Examiner rejected over the Wiecha patent in view of the Ginter patent, applicant submits that the claim "securitizer" is neither taught nor suggested by either of the cited references. The claim securitizer in claims 8 and 11 is more than a so-called firewall that is commonly used to protect networks from outside interference or hacking. Here, the securitizer monitors the secure network including the purchaser account database and the processor to detect any alterations or changes to the stored delivery data. Unlike a firewall, the securitizer will trigger the disabler to disable a particular purchaser identifier or purchaser accounts even if access to the system is the result of a valid purchaser identifier and not as a hack or break-in to the system. In this way, the securitizer is distinct from the common used and commonly known firewall. Accordingly, Applicant submits that claims 8 and 11 and those claims depending therefrom are allowable over the cited references.

Turning now to claims 14-16, although the Examiner gives a reason for why he contends that dependent claims 15 and 16 would not be patentable, the Examiner does not explain the rejection of independent claim 14. Applicant submits that the features of claim 14 are neither taught nor suggested by the cited references and, therefore, independent claim 14 and claims 15 and 16, which depend therefrom, are allowable. For the reasons stated above that Wiecha does not teach or suggest the independent processing system of claim 14 and Ginter does not teach or suggest the disabler, claim 14 is allowable.

The Examiner rejects claims 7, 18, and 19 under 35 U.S.C. § 103(a) as being unpatentable over the Wiecha patent in view Ginter and further in view of U.S. Patent No. 5,890,137 ("Koreeda"). In essence, the Examiner contends that neither the Wiecha patent nor the Ginter patent explicitly discloses having a specific account. Nevertheless, the Examiner contends that the Koreeda patent discloses purchaser account information comprising payment data associated with a purchaser identifier.

First, Applicant notes that claim 7 has been cancelled, without prejudice, and therefore the Examiner's rejection of claim 7 has been obviated. Further, Applicant submits that the

combination of Wiecha in view of Ginter and further in view of Koreeda fails to teach or suggest the claimed features of claims 18 and 19. Moreover, claims 18 and 19, which are dependent from claim 17, are now allowable as being based on an allowable independent claim.

The Newly Submitted Claims 22-24 are Also Allowable

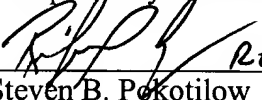
Applicant has submitted new claims 22-24 herewith. Support for the new claims can be found in the Specification as originally filed and no new matter has been added. For the reasons set forth above, Applicant submits that claims 22-24 are in condition for allowance.

Conclusion

Applicant has made a diligent effort to place the Application in condition for allowance and respectfully submit that claims 1-6 and 8-21, and new claims 22-24 in light of the amendments and arguments set forth above, are in condition for immediate allowance. Consequently, if the Examiner cannot issue immediate Notice of Allowance, the Examiner is respectfully requested to contact the undersigned attorney to discuss the outstanding issues.

Any new and additional fees or charges beyond which are stated in said transmittal letter filed concurrently herewith should be charged to Deposit Account No. 19-4709 as necessary.

Respectfully submitted

*for*  REG. NO. 48,874  
Steven B. Pokotilow  
Registration No. 26,405  
Attorney for Applicant  
Stroock & Stroock & Lavan LLP  
180 Maiden Lane  
New York, New York 10038  
(212) 806-5400

## VERSION WITH MARKINGS TO SHOW CHANGES

1. (Amended) A processing system for processing a secure purchase order between a purchaser and a merchant across a public network, the processing system comprising:

a purchaser account database for storing therein purchaser account information for each purchaser, the purchaser account information including at least a purchaser identifier for identifying a particular purchaser, payment data for effecting payment of purchased goods or services, and delivery data associated with said purchaser identifier, said delivery data including at least one delivery address of said purchaser for fulfillment of the purchase order;

a disabler for monitoring the status of the purchaser account information; ~~[and disabling the purchaser account information in response to a monitored change in the purchaser account information; and]~~

a processor for receiving the purchase order from said public network, said purchase order including said purchaser identifier; ~~[and causing said delivery data associated with the purchaser identifier to be communicated to said merchant.]~~

wherein, in response to receipt of the purchase order including the purchaser identifier, the processor retrieves the payment data and the delivery data from the purchaser account database corresponding to the purchaser identifier, transmits the delivery data to the merchant to fulfill the purchase order, and uses the payment data to pay for the purchased goods or services without exposing the payment data to the merchant; and

wherein, in response to a monitored change in the delivery data associated with a particular purchaser identifier, the disabler disables the purchaser identifier such that no purchases can be made using that purchaser identifier.

14. (Amended) A transaction processing service for facilitating the processing of a secure purchase order between a purchaser and a merchant across a public network, the processing service comprising:

a processing system, including:

a purchaser account database for storing therein purchaser account information for each purchaser, the purchaser account information including at least ~~[one of]~~ a

purchaser identifier for identifying a particular purchaser, payment data for effectuating payment of the purchase order, and delivery data associated with said purchaser identifier and containing a delivery address of said purchaser for fulfillment of the purchase order;

a disabler for monitoring the status of the purchaser account database and disabling the purchaser identifier [~~account database~~] in response to a monitored change in the purchaser account information; and

a processor for receiving the purchase order from said public network, said purchase order including said purchaser identifier;

wherein the processor retrieves the delivery data and payment data associated with the purchaser identifier from the purchaser account database and [causing] transmits said delivery data associated with the purchaser identifier to be communicated to said merchant and effectuates payment for the purchase order without exposing the payment data to the merchant.

17. (Amended) A method of facilitating secure transactions between purchasers and merchants across a public network, comprising the steps of:

storing purchaser account information which includes at least payment data for paying for purchased goods and delivery data for delivery of the purchased goods to the purchaser;

issuing a purchaser identifier to a purchaser for use in purchasing goods from a merchant; [~~for identifying particular purchasers;~~

~~storing purchaser account information on a storage device, the purchaser account information including at least the purchaser identifier and delivery data associated with the purchaser identifier on a processing system connected to the public network;~~

~~monitoring the storage device to determine the status of the purchaser account information;~~

disabling the purchaser identifier [~~storage device if the status of the purchaser account information has changed~~] in response to any change in the purchaser account information or if the purchaser account information is accessed by an unauthorized user;

receiving a purchase order ~~[at the processing system]~~ to purchase a product wherein ~~[along with]~~ the purchase order includes the purchaser identifier; [and]

retrieving the delivery data and payment data associated with the received purchaser identifier;

effectuating payment for the purchased product using the payment data without exposing the payment data to the merchant; and

communicating only the delivery data for the purchaser identified by the purchaser identifier to the merchant.

18. (Amended) The method of claim 17, wherein the method further comprises prior to the step of effectuating payment [further comprising the steps of:]

~~[storing purchasing data associated with a respective purchaser identifier corresponding to an ability to pay and method of payment for said particular purchaser;]~~

determining whether ~~[said particular]~~ the identified purchaser can pay for [said] the purchased product; and

if said purchaser is not capable of paying, canceling the purchase order.  
~~[transferring payment to said merchant in accordance with said method of payment.]~~

20. (Amended) A method of facilitating secure transactions between purchasers and merchants across a public network, comprising the steps of:

at a purchaser system having access to a merchant store system:

selecting a product offered for sale by ~~[a=]~~ the merchant, the product being associated with a product identifier;

transmitting [inputting] a purchaser identifier [into] from the purchaser system to the merchant store system; [a purchaser device, the purchaser identifier corresponding to a delivery address stored on a processing system, and the processing system having a disabler for invalidating the purchaser identifier in response to any attempted changes to the delivery address;]

at the merchant store system:

receiving the purchaser identifier;

generating a purchase order for the selected product that includes the purchaser identifier; and

communicating [a] the purchase order [for the product including the product identifier and the purchaser identifier] to the processing system; and

at the processing system:

processing the purchase order to retrieve delivery data and payment data associated with the purchaser identifier; [and]

effectuating payment for the selected product without exposing the payment data to the merchant; and

[upon the purchase order being processed,] communicating [only] the delivery data [address] corresponding to the purchaser identifier to the merchant.

21. (Amended) The method of claim 20, wherein ~~[during said input step]~~ said purchaser is not given an opportunity to change said delivery data ~~[address]~~.